NATIONAL CREDIT UNION ADMINISTRATION
OFFICE OF INSPECTOR GENERAL

AUDIT OF THE
NATIONAL CREDIT UNION ADMINISTRATION'S
MOBILE DEVICE SECURITY CONTROLS

Report # OIG-15-01

January 28, 2015

Inspector General

Released by:

R. William Bruns

R. William Bruns
Deputy Inspector General

W. Marvin Stith, CISA, CICA
Sr. Information Technology Auditor

TABLE OF CONTENTS

EXECUTIVE SUMMARY

We conducted an audit to determine whether NCUA has adequate mobile device security controls to help protect NCUA information and information systems assets.

To accomplish this audit, we conducted fieldwork at NCUA's headquarters in Alexandria, Virginia. We interviewed staff from the NCUA Office of the Chief Information Officer (OCIO). We reviewed NCUA documentation pertaining to the security of mobile devices operating within the NCUA environment. We also reviewed National Institutes of Standards and Technology (NIST) policy and procedure publications and Office of Management and Budget (OMB) policy.

We determined that NCUA policies along with the agency's practices and controls associated with its NCUA-issued mobile devices provide adequate security to protect NCUA information, data and resources. However, we also determined NCUA could improve security of its mobile devices by addressing the following issues:

- NCUA's System Security Plan (SSP) does not adequately address mobile device security controls.

- NCUA could include additional or enhanced policies or controls in its SSP.

In addition, we determined that the controls associated with managing and securing personal mobile devices operating within the NCUA environment did not provide adequate protections over NCUA information, data and resources. Based on the significant security risks associated with this practice, the OIG issued a management letter to the NCUA Office of the Executive Director in November 2014 recommending the agency cease this practice immediately. In response, the agency did immediately prohibit this practice and also disconnected this service. However, we are recommending that NCUA take additional steps in an effort to address NCUA accounts that might still exist on previously connected inactive devices and to address NCUA documentation that users may have downloaded to active or inactive devices that had connected to NCUA's Exchange Server at any time.

Furthermore, we made two recommendations where NCUA could improve the security policies and controls associated with its agency-issued mobile devices to help the agency better protect its information data and resources.

BACKGROUND

Mobile Device Risks

Mobile device (e.g., smartphones, etc.) use has significantly outpaced the use of personal computers. Information technology analysts recently indicated that in 2013, the global shipment of mobile devices was approximately 535 percent more than the shipment of personal computers, and projected that in 2015, shipments of mobile devices would be nearly 618 percent more. The analysts also indicated smart phones will account for 66 percent of all mobile sales in 2014, and projected that number would be 88 percent in 2018.[1] For business users, mobile devices offer significant flexibility and a convenient alternative to laptop computers. In some organizational environments, convenience and new patterns of work have even led to some dependency on mobile devices. This shift from traditional hardware to mobile devices presents a number of challenges and risks that organizations need to address:

Physical Risk. Mobile devices are easily lost or stolen, particularly in public areas. The consequences of lost devices include the compromise of unprotected and transient data. From a security management perspective, the use of measures such as device tracking\location, remote shutdown\wipe, etc. have been implemented to prevent, or at least mitigate, the threat of device loss or theft.

Organizational Risk. Mobile devices have rapidly pervaded enterprises at all levels. They are now available to most users, either through corporate provisioning or Bring Your Own Device (BYOD[2]) arrangements. In terms of data, information and knowledge that exist across the enterprise, many users have privileged access that is often replicated on their mobile devices.

Technical Risk. In general, mobile devices use service-based operating systems with the ability to run multiple services in the background. While early versions of these operating systems were fairly transparent and controllable in terms of activity, more recent versions tend to "simplify" the user interface by restricting the user's ability to change low-level settings. However, data can be intercepted in real time as it is being generated on the device. Examples include forwarding each email sent on the device to a hidden third-party address or retrieving stored data such as a contact list or saved email messages.

Agency Management of Mobile Devices

Centralized management of mobile devices provides agencies with control over agency-issued and employee-owned mobile devices used to access agency information resources. Agencies must manage the configuration and security settings on these devices; however, since agencies have limited control over BYOD devices, agencies are limited in their ability to manage the settings on these employee-owned devices.

[1] TechCrunch – "Gartner: Device Shipments Break 2.4B Units In 2014, Tablets To Overtake PC Sales In 2015". TechCrunch.com. July 6, 2014 < http://techcrunch.com/2014/07/06/gartner-device-shipments-break-2-4b-units-in-2014-tablets-to-overtake-pc-sales-in-2015/>

[2] Bring Your Own Device - a personally-owned mobile device that employees bring to the workplace for use and connectivity on the secure corporate network.

OBJECTIVE, SCOPE AND METHODOLOGY

The objective of this audit was to determine whether NCUA has adequate mobile device security controls to help protect NCUA information and information systems assets.

To accomplish this audit, we conducted fieldwork at NCUA's headquarters in Alexandria, Virginia. We interviewed staff from the NCUA OCIO. We reviewed NCUA documentation pertaining to the security of mobile devices operating within the NCUA environment. We also reviewed NIST policy and procedure publications, and OMB policy.

We conducted this review from October 2013 through January 2014[3] in accordance with generally accepted government auditing standards and included such tests of internal controls as we considered necessary under the circumstances. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. The scope of this audit included assessing the security controls associated with NCUA-provided mobile devices and personal mobile devices allowed to access\sync with NCUA information system assets. We used information on security control settings as well as mobile device inventory data from NCUA's MobileIron[4] Mobile Device Management solution, Apple Restrictions[5] and Microsoft Exchange ActiveSync as applicable. While we assessed the inventory data from these systems to remove errors and duplicate entries and verified some of the controls implemented on the smartphones, we did not test the automated internal controls of these systems. We also relied on interviews to assess the accuracy of the data from these systems and to verify the implementation of other controls.

[3] We delayed the start of fieldwork on this project based on a request from OCIO. In addition, the fieldwork was periodically interrupted due to competing higher priority tasks and projects within the OIG.
[4] MobileIron controls the access of NCUA-issued mobile devices to NCUA's Microsoft Exchange server and integrates NCUA-issued mobile devices with NCUA's mobile operations.
[5] Apple Restrictions are controls that limit or restrict components of the Apple operating system (iOS), which are configured and enforced via MobileIron.

RESULTS

We determined that NCUA policies along with the agency's practices and controls associated with its *NCUA-issued* mobile devices provide adequate security to protect NCUA information, data and resources. However, we also determined NCUA could improve security of its mobile devices by addressing the following issues:

- NCUA's SSP does not adequately address mobile device security controls.
- NCUA could include additional or enhanced policies or controls in its SSP.

In addition, we determined that the controls associated with managing and securing personal mobile devices operating within the NCUA environment did not provide adequate protections over NCUA information, data and resources.

NCUA has been issuing agency-owned mobile devices (e.g., iPhones) to employees and contractors since April 2012 to access the agency's Exchange Server.[6] In addition, since August 2011, NCUA had allowed employees and contractors who have an Exchange account to use their personal mobile devices to access the agency's Exchange Server. However, based on the significant security risks associated with allowing personal devices to operate within the NCUA environment, the OIG issued a management letter to the NCUA Office of the Executive Director in November 2014 recommending the agency cease this practice immediately. In response, the agency immediately prohibited this practice and also disconnected this service. (We address this issue in more detail later in this report).

NCUA's System Security Plan Needs Improvement

We determined NCUA's SSP does not adequately address mobile device security policies, controls and configurations settings. Specifically, NCUA's SSP does not address the agency's policy regarding: types of organizational resources that mobile devices may access; the types of mobile devices permitted to access NCUA's resources; how NCUA provisions mobile devices; or administering the organization's centralized mobile device management servers, updating the policies in those servers, and addressing all other requirements for mobile device management technologies.

NCUA has three different documents that address security policies for its mobile devices. In addition, NCUA uses the MobileIron Mobile Device Management (MDM) solution and Apple Restrictions to implement and monitor policies\settings for its mobile devices. These policies

[6] During the audit, we determined that as of April 3, 2014, NCUA had issued approximately 1,100 iOS mobile devices to employees and contractors to access their Exchange information.

and systems contain varying elements of NCUA's overall mobile device security policies and controls. Specifically:

- *General Support Systems (GSS) SSP* - The security plan provides an overview of the security of the NCUA General Support System (NCUA-GSS) and describes the *controls* and critical elements in place or planned for, based on NIST Special Publication (SP) 800-53, Rev.4 *Security and Privacy Controls for Federal Information Systems.* The SSP documents the current and planned information security controls for the NCUA-GSS and addresses security concerns that may affect the system's operating environment.

- *Mobile Device Security Policy* – This policy establishes security settings and describes security policies that are specific to NCUA-owned mobile devices.

- *NCUA Rules of Behavior*[7] – This document addresses privacy and security obligations and specific computer security controls that must be followed when collecting, maintaining, using, or distributing agency information in electronic or physical form. These "rules" apply to anyone issued an NCUA device and anyone who has access to NCUA data.[8]

- *MobileIron MDM Solution* – MobileIron controls the access of NCUA-issued mobile devices to NCUA's Microsoft Exchange server and integrates NCUA-issued mobile devices with NCUA's mobile operations. It implements NCUA's settings\policy for mobile device Lockdown, Security, Privacy and Syncing.

- *Apple Restrictions* - These are controls that limit or restrict components of the Apple operating system (iOS), which are configured and enforced via MobileIron.

OMB requires agencies to follow NIST SP 800-124, *Guidelines for Managing the Security of Mobile Devices in the Enterprise, Revision 1, June 2013* (NIST Mobile Device Guidelines). NIST Mobile Device Guidelines requires agencies to document mobile device security policy in the agencies' system security plans, and to the extent feasible and appropriate, the policy should be consistent with and complement security policy for non-mobile systems. NIST Mobile Device Guidelines also indicate that the policy should:

- Define which types of the organization's resources may be accessed via mobile devices;

- Define which types of mobile devices are permitted to access the organization's resources;

[7] Every new employee and contractor must agree to the Rules of Behavior and must review and accept them annually thereafter as part of NCUA's Security Awareness and Training.

[8] NCUA's Rules of Behavior indicates that the agency's information security policies are documented in NCUA's Information Security Policy Handbook. However, we noted the Handbook did not address the security of mobile smart devices.

- Define the degree of access that various classes of mobile devices may have, for example, organization-issued devices versus personally-owned devices;

- Define how provisioning of mobile devices should be handled; and

- Address how the organization's centralized mobile device management servers are administered, how policies in those servers are updated, and all other requirements for mobile device management technologies.

In addition, NIST 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* April 2013 (NIST Controls) provides guidelines for selecting and specifying security controls for organizations and information systems with the goal to achieve more secure information systems and effective risk management. NIST Controls indicates: (1) security controls are the safeguards/countermeasures prescribed for information systems or organizations that are designed to protect the confidentiality, integrity, and availability of information that is processed, stored, and transmitted by those systems/organizations; and (2) the use of mobile devices might result in the need for additional security controls and control enhancements not selected in the initial baselines.

Following is our assessment of where NCUA’s SSP (and other mobile device policies) lack mobile device security controls specific to NIST requirements:

- <u>Unsuccessful Logon Attempts (AC-7)</u>: NIST Controls requires agencies to: (1) enforce a limit of consecutive invalid logon attempts by a user during a specified period; and (2) to automatically (a) lock the account for a specified period; (b) lock the account until released by an administrator; or (c) delay next logon prompt when the maximum number of unsuccessful attempts is exceeded.

    - NCUA’s SSP includes the policy to lock NCUA mobile devices after [redacted] consecutive invalid logon attempts. In addition, NCUA implements this security control via its MobileIron MDM solution. However, neither NCUA’s SSP nor its other mobile device policies address delay times between logon attempts. We noted ‘delay times’ is an inherent control within the Apple operating system (See Table 1), which should be documented or referenced in the SSP.

Failed Attempt #	Wait Time [After Attempt]	Total Wait Time
1 - 5	None	None
6	1 Minute	1 Minute
7	5 Minutes	6 Minutes
[redacted]	[redacted]	[redacted]

Table 1: iOS Delay Times between Logon Attempts

- Unsuccessful Logon Attempts | *Purge / Wipe Mobile Device* (AC-7(2)): This control enhancement in NIST Controls requires agencies to purge\wipe information from the mobile devices after a specified number of consecutive, unsuccessful device logon attempts.

  - While NCUA implements a security control via its MobileIron MDM solution to erase data on NCUA mobile devices after [redacted] failed logon attempts, neither NCUA's SSP nor its other mobile device policies address this control.

- Access Controls for Mobile Devices (AC-19): NIST Controls requires agencies to: (a) establish usage restrictions, configuration requirements, connection requirements and implementation guidance for their mobile devices; and (b) authorize the connection of mobile devices to organizational information systems. This control indicates that usage restrictions and specific implementation guidance for mobile devices include, for example: configuration management, device identification and authentication, implementation of mandatory protective software, scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware.[10]

  - This control in the SSP indicates NCUA issues mobile devices to appropriate staff based on manager approval. It also indicates under "Usage Restrictions" that: (1) only pre-configured NCUA-issued *laptops* are authorized to access resources on the internal network; and (2) NCUA-owned…*mobile media devices* may be connected to the Guest wireless network. Under another control (Remote Access (AC-17), the SSP also indicates "Secure VPN access is only available on NCUA-issued laptops…. Remote access is not available for mobile devices such as phones and tablets." However, while the SSP indicates Mobile IRON [sic] is the method of *authenticating* mobile devices, the security policy does not adequately address authorizing these devices to connect to NCUA system(s), i.e., to NCUA's Exchange Server.

[redacted]

[10] This control cautions agencies that the need to provide adequate security for mobile devices goes beyond these requirements.

- The control under NCUA's SSP AC-19 "Configuration & Implementation" indicates that NCUA protects resources through measures such as "whole disk *laptop* encryption, *removable media* encryption, antivirus software, disabled auto-run for *CD/DVD* and *USB media*, and USGB [sic] security baseline configuration." However, the SSP does not address configuration and implementation controls associated with mobile devices. For example:

  - While Microsoft Exchange ActiveSync[11] and the MobileIron MDM solution (e.g., Mobile@Work[12], Apps@Work[13], etc.) have a role in connecting, monitoring and managing NCUA mobile devices within the NCUA environment, NCUA's SSP does not adequately address MobileIron's role and does not address the roles of ActiveSync or Apple Restrictions as they pertain to mobile device connection, configuration or implementation.

  - NCUA's *Mobile Device Security Policy* establishes configuration settings/policy for iPhones specific to: Passcode, Auto Lock, Access on Lock screen[14], Privacy Location Services[15] and Fingerprint features.[16] However, while NCUA has implemented these controls on its mobile devices, the SSP only includes the "Auto Lock" configuration control setting.

  - While NCUA uses the MobileIron MDM solution to implement the controls associated with mobile device "Lockdown," "Security," "Privacy" and "Sync" policies, NCUA has not addressed the majority of the MobileIron security settings within its SSP.[17] For example, NCUA has implemented the following settings for its mobile devices: [redacted]

[11] Microsoft Exchange ActiveSync is a protocol which allows mobile devices to synchronize data with Exchange mailboxes. The protocol synchronizes mail, calendar, contacts, and tasks over the air with Microsoft Exchange Server.

[12] MobileIron's Mobile@Work™ app integrates devices with an organization's mobile operations. It automatically configures devices for access to agency networks and provides access to email, attachments, and other corporate resources.

[13] MobileIron's Apps@Work is an application storefront that manages in-house developed apps and third party business apps that can be delivered to users. The MobileIron Enterprise App Storefront has three primary capabilities: (1) Application Distribution Library; (2) Application Security and Access Control; and (3) Application Inventory.

[14] This control prevents access to the iPhone Control Center from the lock screen.

[15] Location Services allows location-based apps and websites to determine your approximate location.

[16] The document also establishes NCUA's policy for patch management of the devices and its e-mail policy.

[17] The MobileIron MDM settings NCUA provided the OIG included 26 available security controls.

    - NCUA uses Apple's Restrictions to control such actions as prohibiting iOS devices from backing up to the iCloud and from using AirDrop[18] to transfer files. While NCUA does have policy in its Rules of Behavior *informing* users that they are not authorized to use AirDrop or iCloud, NCUA does not include these restrictions or address other "restrictions" in its SSP.

- Access Controls for Mobile Devices | *Full-Device/Container-Based Encryption* (AC-19 (5)): NIST Controls requires agencies to employ either full-device encryption or container encryption to protect the confidentiality and integrity of information on the mobile devices.[19]

    - The "Encryption" annotation under AC-19 of the NCUA SSP only indicates that "All phones are PIN-protected". While the SSP does indicate under other controls – Media Use (MP-7) and Transmission Confidentiality and Integrity (SC-8) – that the iPhone is encrypted, it does not indicate whether the NCUA deploys its mobile devices with full-device encryption or container-based encryption. (We address NCUA's implementation of encryption on the iPhone later in the report.)

- Media Sanitization (MP-6): NIST Controls requires agencies to sanitize *information system media* prior to disposal, release out of organizational control, or release for reuse in accordance with applicable federal and organizational standards and policies.[20]

    - NCUA's Rules of Behavior advises users that all NCUA-issued devices returned at the conclusion of employment will be wiped of all personal data. NCUA staff also indicated they factory reset (i.e., sanitize) every mobile device that users turn-in. However, while the SSP indicates that OCIO will ensure eliminating information from iPhones prior to *re-issuing* them to another user, the SSP does not address sanitization of mobile devices prior to disposal. The SSP does indicate that "All digital storage media used in the GSS environment will be either sanitized or destroyed before release from NCUA custody…Degaussing will be the preferred method." The SSP specifically addresses reimaging[21] workstations and degaussing[22] server hard drives. *Degaussing* and *reimaging* do not apply to mobile devices. Sanitizing a mobile device involves selecting the requisite setting on the device to return it to its factory default state (i.e., factory reset).

[18] AirDrop allows the quick and easy transfer of files from one iPhone to another iPhone or iPad over a secure, ad-hoc Bluetooth and Wi-Fi connection. NCUA indicated this is a prohibited file sharing tool that does not meet the agency's file sharing security requirements.

[19] Container-based encryption provides a more fine-grained approach to the encryption of data/information on mobile devices, including for example, encrypting selected data structures such as files, records, or fields.

[20] Examples of information system media this applies to include media found in scanners, copiers, printers, notebook computers, workstations, network components, and mobile devices.

[21] Reimaging is the process of removing all software on a computer and reinstalling everything. The word reinstall is often used in place of reimage.

[22] This process of degaussing renders the data stored on media such as hard drives and backup tapes completely unreadable.

- Media Use (MP-7): NIST Controls requires agencies to restrict or prohibit the use of specified information systems media on specified information systems\system components using specified safeguards.[23]

  - This control in the NCUA SSP addresses restricting the use of digital media on NCUA *computers*, e.g., thumb drive protections. Regarding *mobile devices*, the SSP indicates only that its "iPhones are encrypted." Considering the functions and capabilities of mobile devices with stored data, NCUA could use this control to address such issues as how the agency facilitates protecting NCUA data from personal use functions and applications (e.g., container-based encryption).

- Transmission Confidentiality and Integrity | *Cryptographic or Alternate Physical Protection* (SC-8 (1)). NIST Controls (SC-8) requires that the information system protect the confidentiality and\or integrity of the transmitted information, which can be accomplished via physical or logical means (e.g., encryption techniques).[24] The control enhancement (SC-8 (1)) requires the information system to implement cryptographic mechanisms to prevent unauthorized disclosure of information and\or detect changes to information during transmission unless otherwise protected.

  - NCUA's SSP provides specific information regarding encryption technology associated with data communications\transmission such as Virtual Private Network (VPN) use, encryption technology associated with Wi-Fi access points and encryption technology associated with email containing PII. The SSP does not provide specific encryption technologies associated with protecting mobile device transmissions, which is actually specified in another NCUA document. Specifically, NCUA completed a "MobileIron Risk Assessment" in April 2014, which indicates: "All communication across the Internet between mobile devices…and MobileIron devices is encrypted using AES 256 bit encryption." The SSP, however, merely indicates that "iPhone mobile devices are PIN-protected and encrypted.

- Usage Restrictions (SC-43): NIST Controls requires agencies to: (1) Establish usage restrictions and implementation guidance for specified information systems[25] components based on the potential to cause damage to the information system if used maliciously; and (2) Authorize, monitor and control the use of such components within the information system.

  - The NCUA SSP does not include this control. However, it would be the ideal control in which to incorporate or at least reference other policies, controls and configuration settings such as: (1) mobile device usage and guidance restrictions from NCUA's

[23] This control applies to mobile devices with information storage capability (e.g., smartphones, tablets).
[24] This applies to all types of information system components from which information can be transmitted, e.g., mobile devices.
[25] Information system components include hardware, software, or firmware components (e.g., Voice Over Internet Protocol, mobile code, digital copiers, printers, scanners, optical devices, wireless technologies, mobile devices).

Rules of Behavior, and (2) control settings from NCUA's MobileIron MDM solution as follows:

- NCUA's Rules of Behavior provides guidance such as users:
  - Should create a strong passcode required for access to mobile devices to prevent unauthorized users from gaining access to NCUA data.
  - Are not authorized to transfer any NCUA content stored on NCUA mobile devices to any other medium not approved by NCUA.
- NCUA's MobileIron MDM solution authorizes, monitors and controls agency-issued mobile devices through such settings as:
  - Password = *Mandatory*
  - Take action if iOS is compromised = *Enabled*. (If an iOS device is jailbroken[26], email would be blocked, in-house apps would be disabled, and NCUA would be alerted and would remove the device from the network.)

NCUA Could Improve the Security of its Mobile Devices

While we determined that NCUA policies and procedures for its NCUA-issued mobile devices provide adequate security to protect NCUA information, data and resources, we believe NCUA could make improvements to better protect the confidentiality, integrity, and availability of NCUA information, data and resources.

As indicated above, NCUA's SSP does not include NIST Controls' Usage Restrictions (SC-43), which we indicated would be an ideal location in which to incorporate or reference usage and guidance restrictions from NCUA's Rules of Behavior and controls implemented via MobileIron. We believe this would also be the ideal location in which to address additional and stronger controls to further improve mobile device security within NCUA's environment. Specifically:

- The Rules of Behavior includes the following policies that NCUA could use to enhance controls to strengthen security of its mobile devices:
  - *Policy* - Users should create a strong passcode required for access to mobile devices to prevent unauthorized users from gaining access to NCUA data.
    - *OIG Discussion* - [redacted]

[26] To jailbreak (or root) a phone circumvents the built-in security and protection of the operating system, opening up the phone to malware and unsupported uses. Jailbroken devices also allow any application to be installed on the phone and malicious applications to steal contacts and corporate data. This inherently makes the mobile device less secure.

[redacted]

- *Policy* - Users are not authorized to transfer any NCUA content stored on NCUA mobile devices to any other medium not approved by NCUA. This includes but is not limited to any commercial cloud storage services (i.e. iCloud, SkyDrive, DropBox, or Office365). Users are not authorized to use AirDrop, a prohibited file sharing tool that does not meet NCUA file sharing security requirements.

  - *OIG Discussion* - According to industry guidance, file sharing apps are the most common blacklisted apps in an enterprise. [redacted]

- *Policy* - Users should not share attachments with non-NCUA applications.

  - *OIG Discussion* - A mobile security concept known as containerization creates an encrypted data store or container on a mobile device. Access to data in the container requires secure authentication independent of any other device setting or restriction. As a result, the contents of the container remain inaccessible unless an authorized user enters valid credentials. Securing data in a container also allows an agency to wipe all business data from a mobile device without affecting personal data or apps. [redacted]

- *Policy* - Users are not authorized to pair mobile devices with Bluetooth devices that allow file transfer or enable Bluetooth if the user does not have a Bluetooth device.

[27] SendAnywhere allows users to quickly and easily send files from their iPhone to their PC or other mobile devices.

[28] MobileIron Docs@Work allows users to work securely with internal documents on their mobile devices by creating an encrypted container in which all internal documents are stored separately from any other content on the mobile device. It is also possible to predefine applications which are allowed to open and modify the documents.

  - *OIG Discussion* - This guidance in NCUA's Rules of Behavior does not adequately address Bluetooth requirements. NIST 800-121 Revision 1, *Guide to Bluetooth Security*, June 2012 indicates a security policy that defines requirements for Bluetooth security is the foundation for all other Bluetooth-related countermeasures. The policy should include: (1) a list of approved uses for Bluetooth, (2) a list of the types of information that may be transferred over Bluetooth networks, and (3) requirements for selecting and using Bluetooth personal identification numbers (PINs), where applicable. We believe NCUA could establish more definitive Bluetooth control guidance.

- *Additional Controls* – We believe NCUA could also add controls to further strengthen security of its mobile devices. For example, neither NCUA's SSP nor any of its other mobile device policies address usage restrictions or guidance pertaining to Quick Response (QR) codes.[29] NIST Mobile Device Guidelines indicate: Mobile devices may use untrusted content - such as QR codes - that other types of devices generally do not encounter. Malicious QR codes could direct mobile devices to malicious websites or could enable a hacker to access messages and GPS, turn on the camera, and listen in on phone conversations. A primary mitigation strategy is to educate users on the risks inherent in untrusted content and to discourage them from accessing untrusted content with any mobile devices they use for work.

Incorporating comprehensive mobile device security policies, controls and configuration settings into NCUA's System Security Plan as required by NIST would help ensure NCUA will continue to effectively, efficiently and consistently protect NCUA information, data and resources from evolving mobile device risks and threats. Also, additional controls as required by NIST and stronger existing controls will help NCUA to more effectively protect NCUA information, data and resources from evolving mobile device risks and threats. Ultimately, this would help mitigate the potential for leakage of confidential or sensitive NCUA data to external unauthorized entities.

Recommendations

We recommend NCUA management:

1. Incorporate NCUA's existing mobile device security policies, controls and configuration settings into the agency's System Security Plan as required by NIST 800-124 and NIST 800-53, Revision 4.

Management Response

OCIO will update the SSP to incorporate all applicable existing security policies, controls and configuration settings, as well as the needed improvements outlined in the report. OCIO will fully address this recommendation by May 31, 2015.

[29] QR codes are specifically designed to be viewed and processed by mobile device cameras.

OIG Response

We concur with management’s planned action

2. Supplement or enhance NCUA’s existing mobile device security policies, controls and configuration settings by addressing the following security measures:

    a. Passcode guidance or controls;
    b. Unauthorized applications;
    c. Container-based encryption;
    d. Bluetooth controls (Per NIST 800-121, Revision 1); and
    e. QR codes

Management Response

OCIO will address the above controls and incorporate them into the updated SSP. OCIO will document and implement the required technical controls and policies by May 31, 2015.

OIG Response

We concur with management’s planned action.

Use of Personal Mobile Devices Increased Security Risks

We determined NCUA's mobile device policies and practices did not adequately address security of personal mobile devices that NCUA allowed its employees and contractors to connect to the NCUA Exchange Server via Microsoft's ActiveSnyc.[30] Specifically, we determined that the controls associated with and available to NCUA to manage personal mobile devices provided very limited assurance that the agency would be able to adequately protect NCUA data, information, and resources.

We determined that as of February 3, 2014, there were approximately 300 personal devices that had connected to NCUA via ActiveSync within the previous 30 days (active devices) and approximately 250 devices that had not connected in more than 30 days (inactive devices). As with the NCUA-issued mobile devices, NCUA email, contacts and calendar items synced to these personal devices. The limited controls significantly increased the risk of the loss or exposure of confidential or privacy-related NCUA information to outside parties. Considering the significance and magnitude of this security risk, we issued a letter to the Office of the Executive Director on November 6, 2014, recommending that NCUA immediately cease this practice. On November 7, 2014, the NCUA Office of the Executive Director issued a letter: (1) notifying users that they were no longer authorized to use their personal mobile devices to sync email from their NCUA accounts; and (2) requiring the users to remove the NCUA account from their devices, which also removes the Exchange information. In addition, NCUA indicated it blocked the access of non-NCUA devices to Microsoft Exchange ActiveSync effective November 21, 2014.

However, since NCUA information could remain on an inactive device, the OIG has concerns that current NCUA employees and contractors might not remember to also remove the accounts from inactive personal devices they may still have access to, if applicable. In addition, while removing the NCUA accounts from active and inactive devices also removes the Exchange information, this action would not remove any agency documentation users may have downloaded to the devices.

Failing to remove the ActiveSync account from both active and inactive personal devices and failing to delete downloaded agency documents from those devices continues to expose NCUA to the risk of leakage of sensitive or confidential agency information.

Recommendation

We recommend that NCUA management:

3. Specifically identify and instruct NCUA employees and contractors that had at any time synced any personal mobile device(s) to the Exchange Server, to remove the NCUA

[30] Personal mobile smart devices that are or have connected to NCUA include Android, iOS, Blackberry and Windows devices.

account from all such devices they may still have access to and to also check for and remove any agency documentation from these devices.

Management Response

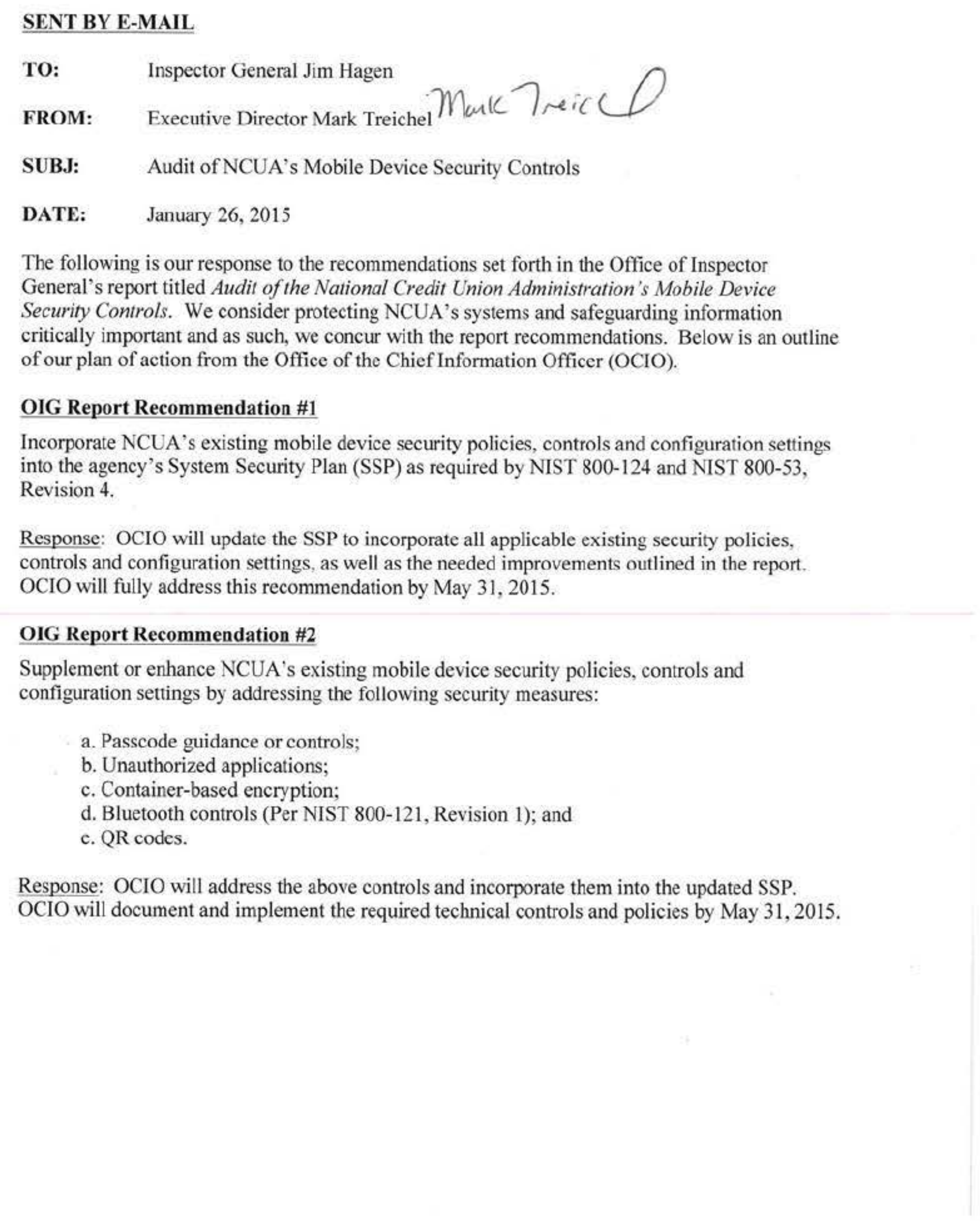
NCUA has taken several proactive steps to neutralize the risks associated with syncing personal devices to NCUA's Exchange Server. A November 7, 2014 memo was issued to all NCUA staff requiring all staff and contractors to remove NCUA accounts from their personal mobile devices. OCIO also disabled ActiveSync for non-NCUA issued mobile devices on November 21, 2014.

By March 31, 2015, management indicated that they will issue guidance to all staff and contractors instructing them to remove any NCUA accounts from all personal devices and to remove any NCUA data from personal devices including mobile phones, personal computers and personal "dropbox-type" applications.

OIG Response

We concur with management's planned action.

Appendix A: NCUA Management Response



SENT BY E-MAIL

TO:	Inspector General Jim Hagen
FROM:	Executive Director Mark Treichel Mark Treichel
SUBJ:	Audit of NCUA's Mobile Device Security Controls
DATE:	January 26, 2015

The following is our response to the recommendations set forth in the Office of Inspector General's report titled *Audit of the National Credit Union Administration's Mobile Device Security Controls*. We consider protecting NCUA's systems and safeguarding information critically important and as such, we concur with the report recommendations. Below is an outline of our plan of action from the Office of the Chief Information Officer (OCIO).

OIG Report Recommendation #1

Incorporate NCUA's existing mobile device security policies, controls and configuration settings into the agency's System Security Plan (SSP) as required by NIST 800-124 and NIST 800-53, Revision 4.

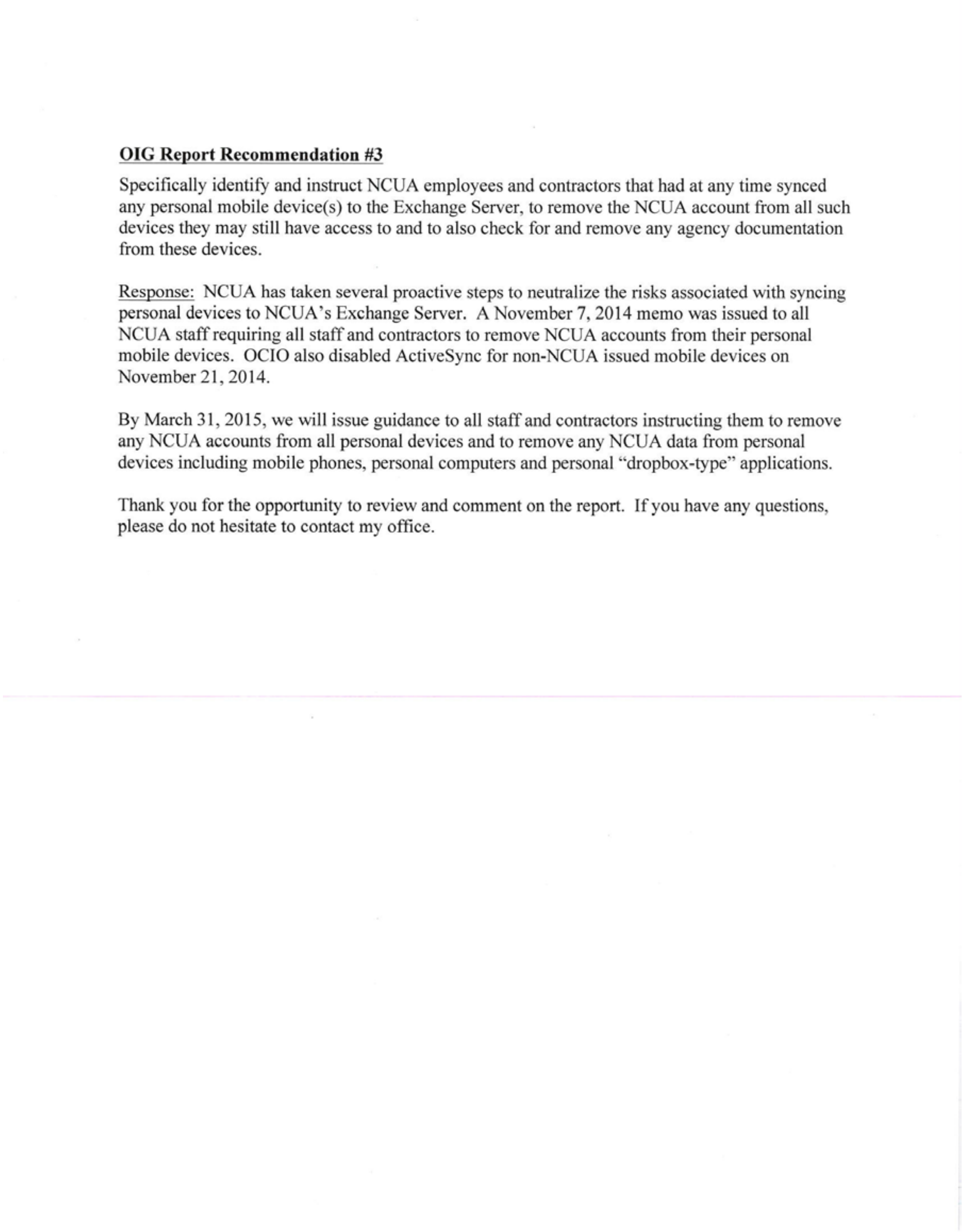
Response: OCIO will update the SSP to incorporate all applicable existing security policies, controls and configuration settings, as well as the needed improvements outlined in the report. OCIO will fully address this recommendation by May 31, 2015.

OIG Report Recommendation #2

Supplement or enhance NCUA's existing mobile device security policies, controls and configuration settings by addressing the following security measures:

a. Passcode guidance or controls;
b. Unauthorized applications;
c. Container-based encryption;
d. Bluetooth controls (Per NIST 800-121, Revision 1); and
e. QR codes.

Response: OCIO will address the above controls and incorporate them into the updated SSP. OCIO will document and implement the required technical controls and policies by May 31, 2015.



OIG Report Recommendation #3

Specifically identify and instruct NCUA employees and contractors that had at any time synced any personal mobile device(s) to the Exchange Server, to remove the NCUA account from all such devices they may still have access to and to also check for and remove any agency documentation from these devices.

Response: NCUA has taken several proactive steps to neutralize the risks associated with syncing personal devices to NCUA's Exchange Server. A November 7, 2014 memo was issued to all NCUA staff requiring all staff and contractors to remove NCUA accounts from their personal mobile devices. OCIO also disabled ActiveSync for non-NCUA issued mobile devices on November 21, 2014.

By March 31, 2015, we will issue guidance to all staff and contractors instructing them to remove any NCUA accounts from all personal devices and to remove any NCUA data from personal devices including mobile phones, personal computers and personal "dropbox-type" applications.

Thank you for the opportunity to review and comment on the report. If you have any questions, please do not hesitate to contact my office.